IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Newport News Division

UNITED STATES OF AMERICA	)	CRIMINAL NO. 4:19cr 84
	)	
v.	)	18 U.S.C. § 1349
	)	Conspiracy to Commit Wire Fraud,
OBINWANNE OKEKE,	)	(Count 1)
	)	
Defendant.	)	18 U.S.C. §§ 1030(b)
	)	Conspiracy to Commit Computer Fraud
	)	(Count 2)
	)	
	)	18 U.S.C. §§ 981, 982
	)	Criminal Forfeiture

INDICTMENT

September 2019 Term - At Newport News, Virginia

GENERAL ALLEGATIONS

At all times relevant to the Indictment:

1. Unatrac Holding Limited, a company headquartered in the United Arab Emirates (UAE), is the export sales office for Caterpillar heavy industrial and farm equipment. In or about the Spring of 2018, Unatrac was victimized in their United Kingdom offices through an email compromise scheme, which ultimately resulted in fraudulent wire transfers totaling nearly $11 million (11 million US Dollars).

2. On or about April 1, 2018, Unatrac's Chief Financial Officer ("CFO") received a phishing email containing a web link, purportedly to the login page of the CFO's online email account hosted by Microsoft Office365. When the CFO opened the link, it instead led him to a phishing web site crafted to imitate the legitimate Office365 logon page. Believing the page to be

real, he entered his login credentials, which were captured by an unknown intruder who controlled the spoofed web page.

3. After capturing the legitimate credentials, the intruder was able to remotely login and access the CFO's entire Office365 account, which included all of his emails and various digital files. Between April 6 and April 20, 2018, the intruder accessed the CFO's account at least 464 times, mostly from Internet Protocol (IP) addresses in Nigeria.

4. With full access to the account, the intruder sent fraudulent wire transfer requests from the CFO's email account to members of Unatrac's internal financial team. The intruder also attached fake invoices to the emails to enhance the credibility of the requests. For many of the invoices, the intruder used content sourced from within the CFO's own account, such as Unatrac logos and preformatted invoice templates, ostensibly to make the invoices appear authentic. Knowing that invoices typically originate from outside the organization, the intruder also apparently sent emails to the CFO's account from an external address, and then forwarded them to the financial team.

5. During the period of unauthorized access, activity logs show that the intruder created or modified email filter rules for the CFO's account on seven occasions between April 10 and April 17, 2018. The rules intercepted legitimate emails to and from employees on the financial team, marked them as read, and moved them to another folder outside the inbox. These rules appeared to have been created in an attempt to hide from the CFO any responses from the individuals to whom the intruder was sending fabricated emails.

6. Unatrac finance staff processed approximately 15 fraudulent payments between April 11 and April 19, 2018. In some cases, several payments were sent to the same account. In total, nearly $11,000,000 (11 million US dollars) was sent, all of which went to overseas accounts.

7. With full access to the Microsoft Office365 account, the intruder was also able to browse the CFO's files hosted by Microsoft's online file storage service OneDrive. The intruder viewed at least 15 of the CFO's files, primarily those relating to tax filings and the CFO's travel schedule. The intruder downloaded one of these files, which contained portions of Unatrac's standard terms and conditions of sale, and sent it to the external email address iconoclast1960@gmail.com.

8. The iconoclast1960@gmail.com was an account subsequently determined to be associated with and used by OBINWANNE OKEKE, the defendant herein. The defendant is a Nigerian citizen and entrepreneur who operated a group of companies known as the Invictus Group.

9. The defendant used the iconoclast1960@gmail.com email account and other accounts to engage with extensive discussions with other conspirators about creating fraudulent web pages, designed to trick unsuspecting users into providing their account credentials.

10. Between at least December 2017 and October 2018, the defendant (using the iconoclast1960@gmail.com email address) and another individual discussed over e-mail specific details about how to create fraudulent web pages that would capture users' email and password credentials. In order to demonstrate and test their web designs, the iconoclast1960@gmail.com and other accounts also sent each other copies of code used to create the fraudulent web pages.

The defendant and other individuals acted to compile collected credentials of others for use in acts of fraud.

11. Among these credentials were passwords of accounts belonging to victims located within the Eastern District of Virginia. Emails dated January 17, 2018 contained the passwords for victims in Mechanicsville, Virginia and Midlothian, Virginia. An email dated January 18, 2019 contained a password for a victim in Richmond, Virginia, and an email dated February 26, 2018 contained a password for a victim in Ashburn, Virginia. The capture of these passwords was facilitated by wire communications affecting interstate commerce between the Eastern District of Virginia and locations outside Virginia.

12. Other email accounts that were linked to or corresponded with conspirators' accounts engaged in fraudulent schemes targeting individuals and businesses in the Eastern District of Virginia and elsewhere from the time period beginning in at least 2015.

COUNT ONE

THE GRAND JURY CHARGES THAT:

1. The Grand Jury realleges and incorporates by reference the allegations contained the General Allegations section as if fully set forth herein.

2. Beginning on a date unknown to the Grand Jury, but believed to be in or about 2015, and continuing until in or about at least 2019, the exact dates being unknown to the Grand Jury, in the Eastern District of Virginia and elsewhere, OBINWANNE OKEKE, the defendant herein, and others known and unknown to the Grand Jury, did knowingly and willfully combine, conspire, and agree with each other and others known and unknown to the Grand Jury, to knowingly devise and intend to devise a scheme and artifice to defraud and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, for which the defendants and conspirators transmitted and caused to be transmitted by means of wire communications in interstate commerce certain writings, signs, signals and sounds, for the purpose of executing the scheme and artifice, in violation of Title 18, United States Code, Section 1343.

WAYS, MANNER AND MEANS OF THE CONSPIRACY

The ways, manner and means by which the foregoing objectives of the conspiracy to commit wire fraud were to be accomplished included, but were not limited to, the following:

3. The primary purpose of the conspiracy was for the conspirators to obtain funds through fraudulent means by engaging in fraudulent business email compromise, phishing and other computer-based schemes.

4. It was a part of the conspiracy and the scheme and artifice that conspirators sent phishing emails to one or more businesses in an effort to obtain login credentials of employees.

5. It was further a part of the conspiracy and the scheme and artifice that the conspirators obtained legitimate credentials of other individuals that the conspirators then used to commit fraudulent acts targeting other businesses and individuals in order to obtain money and other property, including, but not limited to, accessing protected computers without authorization, sending fraudulent wire transfer requests, using fake invoices and viewing and downloading files belong to other individual and business victims.

6. It was further a part of the conspiracy and the scheme and artifice that the conspirators unlawfully obtained funds belonging to other individuals and/or business entities and caused the transfer of funds to accounts controlled by the conspirators.

7. It was further a part of the conspiracy and the scheme and artifice that the conspirators corresponded with one another via electronic mail.

8. It was further a part of the conspiracy and the scheme and artifice that the conspirators worked to create fraudulent web pages that would capture victims' email and password credentials for use in the aforementioned fraudulent activity.

9. It was further a part of the conspiracy and the scheme and artifice that the conspirators obtained and complied credentials of hundreds of victims, including victims in the Eastern District of Virginia.

10. It was further a part of the conspiracy and the scheme and artifice that the conspirators engaged in and caused wire communications affecting interstate and foreign

commerce between the Eastern District of Virginia and locations outside of the Commonwealth of Virginia.

(In violation of Title 18, United States Code, Sections 1349 and 1343.)

COUNT TWO

THE GRAND JURY FURTHER CHARGES THAT:

1. The Grand Jury realleges and incorporates by reference the allegations contained in the General Allegations section and in Paragraphs 3 through 10 of the Ways, Manner and Means Section of Count One as if fully set forth herein.

2. On or about ~~the dates set forth below~~ 2015 through 2019, within the Eastern District of Virginia and elsewhere, OBINWANNE OKEKE, the defendant herein, and others known and unknown to the Grand Jury, did knowingly and willfully combine, conspire, and agree with each other and others known and unknown to the Grand Jury to commit the following offenses against the United States:

(a) To knowingly and with the intent to defraud, access a protected computer without authorization and exceed authorized access of a protected computer and by means of such conduct furthered the intended fraud and obtain something of value other than use of the computer, in violation of Title 18, United States Code, Section 1030(a)(4); and

(b) To knowingly and with the intent to defraud traffic in any password or similar information through which a computer may be accessed without authorization affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1030(a)(6).

(In violation of Title 18, United States Code, Section 1030(b).)

CRIMINAL FORFEITURE

THE GRAND JURY FURTHER FINDS PROBABLE CAUSE THAT:

1. The defendant, if convicted of any of the violations alleged in Counts One and Two of this Indictment, shall forfeit to the United States, as part of the sentencing pursuant to Federal Rule of Criminal Procedure 32.2, any property, real or personal, which constitutes or is derived from proceeds traceable to the violation.
2. The defendant, if convicted of the violation alleged in Count Two of this Indictment, shall forfeit to the United States, as part of the sentencing pursuant to Federal Rule of Criminal Procedure 32.2, any personal property that was used or intended to be used to commit or to facilitate the commission of the violation.
3. If any property that is subject to forfeiture above is not available, it is the intention of the United States to seek an order forfeiting substitute assets pursuant to Title 21, United States Code, Section 853(p) and Federal Rule of Criminal Procedure 32.2(e).
4. The property subject to forfeiture includes, but is not limited to, the following property:
    a. A monetary judgment in the amount of not less than $11,000,000 representing the proceeds of Counts One and Two; and
    b. Emerald cut engagement ring with small accent diamonds seized from the defendant on August 6, 2019.

(In accordance with Title 18, United States Code, Sections 981(a)(1)(C) and 1030(i)(1); and Title 28, United States Code, Section 2461(c)).

UNITED STATES v. OBINWANNE OKEKE, 4:19cr 84

A TRUE BILL:

REDACTED COPY

_____
FOREPERSON

G. ZACHARY TERWILLIGER
UNITED STATES ATTORNEY

By: _____

Brian J. Samuels
Assistant United States Attorney
Virginia State Bar No. 65898
Fountain Plaza Three, Suite 300
721 Lakefront Commons
Newport News, Virginia 23606
Tel. (757) 591-4000
Fax: (757) 591-0866